Proceedings of the 11th World Congress on Electrical Engineering and Computer Systems and Sciences (EECSS'25)
Paris, France - August, 2025
Paper No. CIST 124
DOI: 10.11159/cist25.124

Enhancing Privacy and Usability in Blockchain Traceability Systems

Ali Al Maqousi[1], Mohammad Alauthman[2]
[1]Department of Information Security, University of Petra
Amman, Jordan
amaqousi@uop.edu.jo
[2]Department of Information Security, University of Petra
Amman, Jordan
mohammad.alauthman@uop.edu.jo

Abstract **-** Blockchain technology has emerged as a promising solution for improving traceability across global supply chains, offering tamper-proof records and increased transparency. However, concerns related to data privacy, confidentiality, and interoperability continue to hinder widespread adoption. This paper proposes a comprehensive framework addressing these key challenges by combining privacy-preserving techniques—such as permissioned ledgers, zero-knowledge proofs, and verifiable credentials—with industry-driven data standards (GS1 EPCIS, W3C Verifiable Credentials). We first review the landscape of blockchain traceability solutions and outline critical requirements from regulatory and operational perspectives. Next, we detail our proposed privacy-preserving and interoperable architecture, incorporating off-chain storage, role-based permissions, and selective disclosure mechanisms to accommodate the diverse needs of modern supply chains. We illustrate these concepts through a high-level system design, accompanied by implementation considerations. Our evaluation highlights that successful adoption depends on carefully balancing transparency and confidentiality, supplemented by robust governance structures and standard APIs. The paper concludes by discussing future directions for blockchain traceability, emphasizing scalability, user-centric design, and cross-chain interoperability as critical enablers of a global, privacy-preserving supply chain ecosystem.

Keywords**:** Blockchain, Supply Chain, Traceability, Privacy, Interoperability, Zero-Knowledge Proofs, Verifiable Credentials.

1. Introduction

Global supply chains have grown increasingly complex and fragmented, with products often passing through multiple intermediaries before reaching end consumers. In parallel, regulators and consumers demand higher standards of transparency, particularly for food safety and pharmaceutical authenticity. Consequently, companies are exploring blockchain technology to create immutable, secure traceability systems that track products from origin to destination [1]–[3]. Blockchain's distributed ledger mechanism ensures tamper-proof recording of supply chain events, enabling faster audits and recalls while building consumer trust.

Despite these benefits, the adoption of blockchain in supply chains has been slow due to concerns over privacy, confidentiality, and system usability [1], [4]. Supply chain actors may be unwilling to share commercially sensitive data (e.g., pricing, supplier relationships) on a shared, potentially transparent ledger [3], [5]. Moreover, many early blockchain traceability pilots relied on public blockchains where transaction details were visible to all participants [6]. This approach raises fears about revealing business secrets, thereby creating significant barriers for industry stakeholders to collaborate openly.

To address these concerns, research has focused on integrating privacy-preserving cryptographic techniques such as zero-knowledge proofs (ZKPs) [6]–[8], anonymization protocols [8], and off-chain data storage approaches [9], [10]. In addition, real-world implementations like the MediLedger project have demonstrated that permissioned networks with strong confidentiality guarantees can meet regulatory requirements while protecting sensitive business data [14]. However, these solutions also highlight the importance of interoperability and seamless integration with existing enterprise systems [2], [5], [11]. Without standardized data models or robust cross-chain communication protocols, supply chain stakeholders risk operating in siloed blockchain systems, undermining the end-to-end visibility necessary for compliance and consumer assurance [12], [18].

This paper addresses these challenges by proposing a comprehensive privacy-preserving framework for blockchain-based supply chain traceability that leverages emerging standards (e.g., W3C Verifiable Credentials, GS1 EPCIS) to ensure

interoperability and usability. We integrate state-of-the-art cryptographic mechanisms, permissioned ledger design, and open data standards to enable selective data sharing and a flexible approach to collaboration. We provide four tables summarizing key privacy technologies, standards, adoption barriers, and critical success factors. Three illustrative figures (in Mermaid code) detail the high-level architecture, zero-knowledge proof interactions, and cross-chain interoperability approach.

The remainder of the paper is organized as follows. Section II synthesizes related work on blockchain-based supply chain traceability, privacy solutions, and interoperability standards. Section III presents our proposed framework, describing the privacy-preserving architecture and relevant protocols. Section IV discusses implementation considerations and a conceptual workflow, including zero-knowledge proof examples. Section V provides a broader discussion of the challenges and future directions, and Section VI concludes the paper with final remarks.

2. Related Work

Blockchain's potential to improve supply chain traceability has been extensively explored in the literature. Early studies identify regulatory compliance, data standards, and privacy as key prerequisites for blockchain-based traceability in agri-food supply chains [1], [17]. Government and industry reports similarly highlight the need to protect confidential business data and ensure interoperability for efficient deployment [2], [3]. Industry consortia have also pushed for open standards to enable cross-platform data exchange [5], [16].

2.1. Privacy-Preserving Approaches

One of the barriers to adoption of blockchain traceability is fear of exposing information that is sensitive, such as sourcing relationship, transaction prices [1] and [3] and [19]. But privacy preserver techniques have been developed by researchers. The frameworks of zero-knowledge proof permit the participants to prove the transaction correctness while hiding the fundamental data. Maintaining confidentiality while preserving data integrity can also be done via off chain storage solutions in which only keyed references are stored on chain [9],[10]. A different approach is to anonymize identities with cryptographic protocols so that it is not possible for users to join together multiple events in the same way to identify an actor. Together, these create a system by which stakeholders have control over their own proprietary data as well as benefit from an immutable ledger.

2.2. Interoperability for Multi-Stakeholder Ecosystems

Supply chains often involve multiple actors with varying software infrastructures. Consequently, interoperable blockchain solutions are essential for widespread adoption [5], [18]. The W3C Verifiable Credentials standard [4] enables the issuance of cryptographically verifiable attestations that can be selectively disclosed. This aligns with GS1 data models like EPCIS, which define event structures and common vocabularies for supply chain information [5], [10]. Industry deployments such as IBM Food Trust and SAP traceability platforms have demonstrated that common identifiers and open APIs can enable partial data sharing across different blockchains [16]. Meanwhile, advanced approaches allow a product's history to be tracked even when crossing from one blockchain to another [12], [18].

2.3. Real-World Implementations and Lessons

Several case studies highlight the need for privacy, usability, and governance in practical blockchain traceability. TradeLens, a shipping-focused blockchain, found that data permissioning and open standards were central to building trust among competing stakeholders [13]. Similarly, the MediLedger project for pharmaceutical traceability proved that permissioned Ethereum networks combined with zero-knowledge proofs could meet the Drug Supply Chain Security Act (DSCSA) standards without exposing sensitive business data [14]. In agriculture, multiple studies emphasize user-friendly solutions and integration with existing ERP systems, especially for smallholder farmers [9], [17], [20]. The consistent theme across these efforts is that technical solutions must be accompanied by sound governance, user-centric design, and industry collaboration on standards to ensure success.

3. Proposed Framework

Informed by the research and lessons above, we propose a blockchain-based traceability framework that aims to reconcile transparency with privacy while providing a high degree of interoperability. Our framework integrates four core components: (1) a permissioned blockchain network for immutable recording, (2) cryptographic privacy techniques including zero-knowledge proofs, (3) an off-chain storage and selective disclosure layer, and (4) standardized data models and APIs.

3.1. System Architecture

Figure 1 (in Mermaid code) provides a high-level overview of our architecture, detailing how supply chain actors, data storage, cryptographic services, and blockchain nodes interconnect. The objective is to ensure that while each product's provenance can be traced, sensitive details remain visible only to authorized parties.

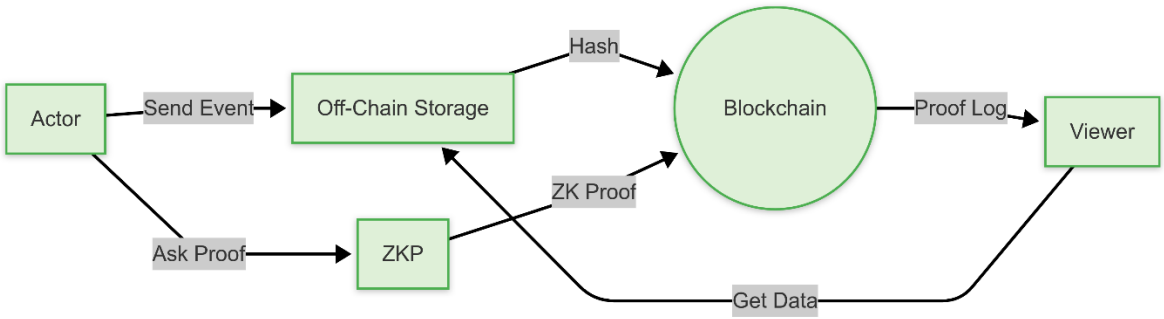

Fig. 1. High-level framework architecture showing off-chain storage, ZKP services, and permissioned blockchain for secure, privacy-preserving traceability.

1. **Permissioned Blockchain Layer:** We adopt a consortium or permissioned blockchain architecture (e.g., Hyperledger Fabric) where only vetted participants can operate nodes, thus mitigating many privacy concerns [2], [10]. This blockchain stores hashes of supply chain events (e.g., shipping, inspections) and cryptographic proofs rather than full data.
2. **Off-Chain Storage:** Detailed data is stored in off-chain databases, which could be a distributed file system like IPFS [9] or a secure cloud repository. Records are referenced on-chain via their hashes, preventing unauthorized entities from accessing sensitive information.
3. **Zero-Knowledge Proof Services:** ZKP protocols (such as zk-SNARKs or bulletproofs) enable supply chain participants to validate or audit product claims without revealing the underlying data [7], [15]. This mechanism can verify conditions (e.g., temperature logs, certifications) while preserving confidentiality.
4. **Selective Disclosure & Access Control:** Role-based permissions define which actors can view which data fields, while verifiable credentials offer a standardized method to confirm identity or other attributes without revealing more information than necessary [4], [5].

3.2. Privacy and Confidentiality Mechanisms

Table I summarizes the primary techniques employed to ensure privacy at different system layers.

Table I: Key Privacy Mechanisms

	Description	Layer
Off-chain Storage	Sensitive data is kept off-chain, accessible only via authorized queries	Data layer
Hashed On-Chain Records	On-chain entries store only hashes or encrypted references	Blockchain layer
Zero-Knowledge Proofs	Enables proof of data integrity/compliance without revealing raw data	Cryptographic layer
Verifiable Credentials	Selective disclosure of identity and product attributes	Identity layer
Role-based Access	Restricts who can see or modify certain data fields	Application layer

1. Off-chain Storage & Encryption: The raw data—such as shipping documents, temperature logs, or supplier details—is encrypted using public-key cryptography, with decryption keys maintained by authorized actors. This prevents unauthorized parties on the network from accessing sensitive information [9], [10].
2. Zero-Knowledge Proof Modules: Each participant can generate cryptographic proofs to demonstrate compliance with regulations or attest to product quality [6], [7]. This approach substantially reduces the risk of data leakage, as only the proof (not the underlying data) is posted to the blockchain.
3. Selective Disclosure: Using W3C Verifiable Credentials, participants can present only the relevant attributes (e.g., organic certification) to interested parties. This ensures compliance with privacy regulations and fosters trust among participants [4], [5].

3.3. Interoperability Framework

Given the diversity of platforms that may be used by different organizations, interoperability is essential for end-to-end visibility. Our framework leverages open data formats like GS1 EPCIS for event records [5], [10] and W3C Verifiable Credentials for identity attributes [4], [11]. Additionally, cross-chain communication protocols can be incorporated if an asset transitions from one ledger to another [12], [18].

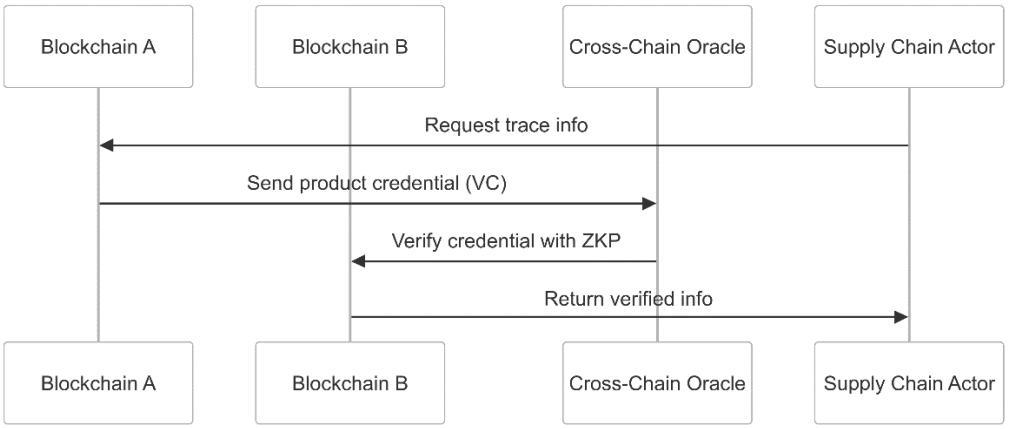

Fig. 2. Cross-chain interoperability via verifiable credentials and oracles. A credential is verified across multiple blockchains without revealing underlying data.

3.4. Governance Model

Table II describes the governance elements essential for maintaining trust and ensuring consistent privacy policies across consortium members.

Table II: Governance Model Components

	Description
Consortium Membership	Defines eligibility, onboarding processes for new members
Data Sharing Policies	Establishes rules for data access, usage, retention
Smart Contract Management	Governs deployment, updates, and versions of chaincode
Regulatory Compliance Verification	Ensures alignment with regional/international laws (e.g., DSCSA, GDPR)
Dispute Resolution	Mechanisms for handling disputes or data conflicts

A robust governance structure assures participants that data-sharing rules and business logic will be enforced consistently [1], [13], [14]. This includes legal agreements that specify usage rights, responsibilities, and recourse in case of misuse or non-compliance.

4. Implementation Details

4.1. Workflow and Interaction Model

To illustrate how the framework could operate in practice, we outline a simple scenario of a multi-tier agri-food supply chain. At each stage, participants generate events, store data off-chain, and register hashed references on the blockchain along with relevant zero-knowledge proofs.

1. Production Stage (Farm): The farm records planting, pesticide usage, and harvest data. These details remain off-chain, but a hashed reference is uploaded to the permissioned blockchain. The farm also obtains verifiable credentials that attest to certifications (e.g., organic labeling) [19].
2. Transport and Warehousing: Logistics partners record temperature and location data using IoT devices. To preserve privacy, only the device's authenticated status and hashed sensor readings appear on-chain [9], [10]. Zero-knowledge proofs can demonstrate compliance (e.g., "temperature stayed below 5°C") without revealing exact logs [6], [7].
3. Processing and Packaging: Manufacturers add processing events. When combining ingredients or components, they verify upstream proofs to ensure authenticity or compliance.
4. Retail and Consumer Access: Retailers verify product provenance via a front-end portal. If consumers want to confirm an organic claim, the system uses verifiable credentials and a zero-knowledge proof to show compliance without exposing the entire audit history [4].

Table III outlines typical data fields at each stage and their on/off-chain representation.

Table III: Example Data Mapping

	Stage	**Key Data Fields**	**On-Chain**	**Off-Chain**
Farm	Production	Harvest date, pesticide usage	Hash of production record	Detailed pesticide usage log, certifications

Transport	Shipping	Temperature logs, route	Hash of sensor readings	Encrypted sensor data, IoT device signature
Processor	Transformation	Batch composition, QA tests	Batch-level proof hashes	Detailed QA data, manufacturing logs
Retail	Distribution	Final packaging, ID labels	Reference to final credentials	Consumer-facing credential (organic, fair-trade)

4.2. Zero-Knowledge Proof Example

Consider a requirement to prove a temperature never exceeded a threshold. Traditional solutions might publish continuous sensor data on-chain, which reveals operational details. Our zero-knowledge approach only publishes a proof that the data remained below 5°C for the entire journey. Figure 3 shows a simplified sequence in Mermaid code.

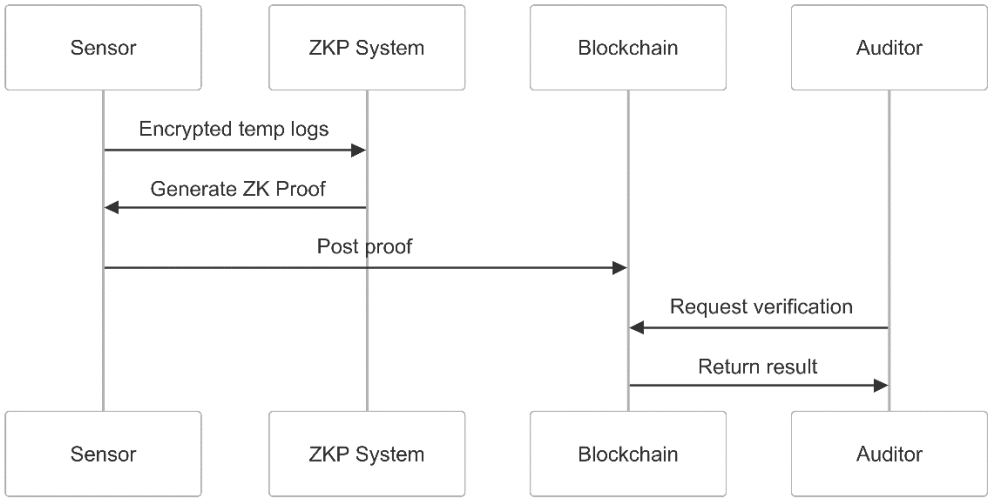

Fig. 3. ZKP-based temperature compliance checking without revealing actual sensor readings.

By leveraging cryptographic proofs, sensitive operational data remains off-chain, and only the success/failure of the validation is visible. This approach is widely applicable to many supply chain compliance checks, including verifying authorized transactions, validating certifications, and more [6]–[8], [14].

4.3. Prototype and Tools

- An implementation could be built using:
- Hyperledger Fabric (for permissioned ledger, chaincode) [10]
- IPFS or other distributed storage for off-chain data references [9]
- zk-SNARK Libraries (e.g., ZoKrates, Libra) for zero-knowledge proof generation [7]
- W3C Credential Libraries (e.g., Hyperledger Indy, Aries) to implement verifiable credential issuance and selective disclosure [4], [11]

While performance constraints of ZKPs remain a concern, advances in polynomial-based proofs and hardware acceleration have significantly improved feasibility for enterprise supply chains [7], [8].

5. Discussion

5.1. A. Balancing Transparency with Privacy

One of the main tensions in blockchain traceability is reconciling consumer/regulatory demands for transparency with the need for trade secret protection [1], [3], [19], [20]. By integrating selective disclosure, zero-knowledge proofs, and permissioned ledgers, our framework aims to provide transparency at a macro-level (the product journey is verifiable) while concealing sensitive commercial data at a granular level.

5.2. B. Interoperability and Standards Adoption

Cross-industry adoption depends on seamless data exchange among heterogeneous systems. Hence, the use of GS1-compliant product identifiers and standardized EPCIS event structures ensures consistent data semantics [5], [10]. W3C Verifiable Credentials further unify identity management and product claims, enabling interoperability across distinct blockchain implementations and cloud services [4], [11], [16].

5.3. C. Governance and Ecosystem Coordination

A robust governance model is crucial. Platform operators must address membership rules, dispute resolution, and data ownership. Several large-scale initiatives, including TradeLens and MediLedger, revealed that ecosystem-wide trust cannot rely solely on technology; off-chain policies and transparent governance are also essential [13], [14].

5.4. D. Scalability and Performance Considerations

Privacy-preserving techniques like zero-knowledge proofs can be computationally intensive. Ongoing research focuses on improving performance, for example through polynomial commitment schemes or specialized hardware [7]. Off-chain storage also mitigates blockchain bloat but introduces complexity in data retrieval and key management [9], [10]. Achieving high throughput suitable for global supply chains remains an area of active investigation.

5.5. E. Future Research Directions

While the proposed framework addresses key usability and privacy challenges, further work is needed to:

1. **Optimize ZKP performance** for real-time supply chain events.
2. **Enhance cross-chain operations** to ensure products can migrate between blockchains seamlessly without duplicating data or losing traceability [12], [18].
3. **Develop user-friendly interfaces** that abstract away complex cryptography and guide non-technical supply chain stakeholders [17], [20].
4. **Standardize privacy-compliance** for multiple regulatory regimes (GDPR, DSCSA) to reduce legal uncertainties [14], [15].

6. Conclusion

This paper presented a comprehensive framework for privacy-preserving, interoperable blockchain-based supply chain traceability. Drawing on existing literature, we identified critical barriers to adoption—data confidentiality, system usability, and cross-platform interoperability—and proposed a layered architecture that integrates permissioned ledgers, off-chain storage, zero-knowledge proofs, and W3C verifiable credentials. By adopting open data standards (GS1 EPCIS) and robust governance structures, our solution balances the need for transparency with the requirement to protect business-sensitive information.

The framework's value lies in enabling stakeholders to share validated, tamper-proof evidence of product journeys, origin claims, and regulatory compliance without exposing proprietary data. This design can address concerns in diverse sectors—agri-food, pharmaceuticals, fashion, and beyond—where trust and confidentiality are paramount. Future work will focus on accelerating cryptographic proofs, refining interoperability protocols, and supporting user-friendly tooling to

broaden participation. Overall, we posit that standardized, privacy-preserving architectures will be pivotal in shaping the next generation of digital supply chain networks.

References

[1] K. Behnke and M. F. W. H. A. Janssen, “Boundary conditions for traceability in food supply chains using blockchain technology,” Int. J. Inf. Manage., vol. 52, Art. 101969, 2019.

[2] K. Stouffer, M. Pease, J. Lubell, E. Wallace, H. Reed, V. L. Martin, S. Granata, A. Noh, and C. Freeberg, *Blockchain and related technologies to support manufacturing supply chain traceability*, vol. NISTIR 8419. National Institute of Standards and Technology, 2022.

[3] World Economic Forum, “Inclusive Deployment of Blockchain for Supply Chains Part 4 – Protecting Your Data,” White Paper, 2019.

[4] World Wide Web Consortium (W3C), “Verifiable Credentials Data Model 1.1,” W3C Recommendation, Mar. 2022.

[5] GS1, “Draft White Paper on Verifiable Credentials and End-to-End Traceability,” ver. 0.4, Apr. 2022.

[6] J. Li, Z. Wang, S. Guan, and Y. Cao, "ProChain: A privacy-preserving blockchain-based supply chain traceability system model," *Computers & Industrial Engineering*, vol. 187, p. 109831, 2024.

[7] J. Z. Nasri and H. Rais, “zk-BeSC: Confidential Blockchain Enabled Supply Chain Based on Polynomial Zero-Knowledge Proofs,” in Proc. IWCMC 2023, 2023.

[8] M. El Maouchi, O. Ersoy, and Z. Erkin, “DECOUPLES: A decentralized, unlinkable and privacy-preserving traceability system for the supply chain,” in Proc. ACM BCC ’19, 2019.

[9] Q. Yao and H. Zhang, “Improving Agricultural Product Traceability Using Blockchain,” Sensors, vol. 22, no. 9, p. 3388, 2022.

[10] L. Li, H. Qu, H. Wang, J. Wang, B. Wang, W. Wang, J. Xu, and Z. Wang, "A blockchain-based product traceability system with off-chain EPCIS and IoT device authentication," Sensors, vol. 22, no. 22, p. 8680, 2022

[11] M. T, K. Makkithaya and N. V G, "A Blockchain-Based Credentials for Food Traceability in Agricultural Supply Chain," 2023 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER), Mangalore, India, 2023, pp. 19-24, doi: 10.1109/DISCOVER58830.2023.10316706.

[12] Y. Mezquita, B. Podgorelec, A. B. Gil-González, and J. M. Corchado, "Blockchain-based supply chain systems, interoperability model in a pharmaceutical case study," *Sensors*, vol. 23, no. 4, p. 1962, 2023.

[13] M. Jovanovic, N. Kostić, I. Sebastian, and T. Sedej, “Managing a blockchain-based platform ecosystem for industry-wide adoption: The case of TradeLens,” Technol. Forecast. Soc. Change, vol. 184, Art. 121981, Nov. 2022.

[14] MediLedger Project (Chronicled Inc.), “MediLedger DSCSA Pilot Project: Final Report to the FDA,” Feb. 2020.

[15] Circularise, “Traceability with privacy: Enabling a circular economy with blockchain,” Circularise Blog, Aug. 17, 2023.

[16] E. Cosgrove, “SAP, IBM Food Trust, GS1 move toward food supply chain traceability with interoperability test,” Supply Chain Dive, 11 Jun. 2020.

[17] A. Kamilaris, A. Fonts, and F. X. Prenafeta-Boldú, “The rise of blockchain technology in agriculture and food supply chains,” Trends Food Sci. Technol., vol. 91, pp. 640–652, 2019.

[18] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," ACM Comput. Surv., vol. 54, no. 8, pp. 1–41, 2021.

[19] A. Badhwar, S. Islam, and C. S. L. Tan, "Exploring the potential of blockchain technology within the fashion and textile supply chain with a focus on traceability, transparency, and product authenticity: A systematic review," *Frontiers in Blockchain*, vol. 6, p. 1044723, 2023.

[20] L. Francisco and D. Swanson, “The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency,” Logistics, vol. 2, no. 1, p. 2, 2018.